

暗号資産取引規制におけるブロックチェーンに対する攻撃の位置付けと想定される対応事項

PwC Japan有限責任監査法人
ガバナンス・リスク・コンプライアンス・
アドバイザリー部
パートナー 竹内 秀輝



PwC Japan有限責任監査法人
ガバナンス・リスク・コンプライアンス・
アドバイザリー部
マネージャー 安嶋 建



はじめに

ブロックチェーンは暗号資産の技術的基盤として用いられており、ブロックチェーンに対する攻撃は暗号資産の価格形成や暗号資産取引の公正性を害する行為として、暗号資産市場に重大な影響を与える可能性があります。

2017年に暗号資産に関する規制が資金決済法に追加されて以降、ブロックチェーンに対する攻撃は暗号資産交換業者等が管理する利用者資産の安全性や業務の適正性を脅かすものと位置付けられ、主として暗号資産交換業者（暗号資産取引所および暗号資産販売所）におけるリスク管理の対象として扱われてきました^{※1}。

その後、2026年7月23日には「金融商品取引法及び資金決済に関する法律の一部を改正する法律」が公布され^{※2}、暗号資産の取引に適用される規制内容は資金決済法から金融商品取引法に移管されることになりました。また、併せて、従来「暗号資産交換業」^{※3}と位置付けられてきた、暗号資産の売買または他の暗号資産との交換等の業務は特定暗号資産の引受け等の業務とともに「暗号資産取引業」^{※4}へと位置付けが変わり、これを行う事業者は「暗号資産交換業者」^{※5}から「金融商品取引業者」^{※6}へと位

置付けが変更され、より広範な規制が適用されることとなりました。

さらに、暗号資産に係る不公正取引規制の導入は、ブロックチェーンに対する攻撃が不公正取引の問題にもなり得ることを示しています。このような状況において、暗号資産取引業を行う金融商品取引業者が犯罪と評価され得る行為に対して適切な対応を行わないことは、規制上求められる態勢整備上の問題のみならず、レピュテーションの深刻な悪化にもつながりかねません。

本稿では、日本において今般導入された暗号資産に係る不公正取引規制を前提として、ブロックチェーンに対する攻撃の法規制上の扱いを整理するとともに、PwCによる支援の経験を踏まえて暗号資産取引業を行う金融商品取引業者において求められる実務対応を示します。

なお、文中の意見は筆者の私見であり、PwC Japan有限責任監査法人および所属部門の正式見解ではないことをお断りしておきます。

1 ブロックチェーンが攻撃される背景

本稿で想定している「ブロックチェーンに対する攻撃」とは、暗号資産の記録、承認、移転の基盤となる分散型台帳またはその周辺インフラに対して、不正または不当な影響を与える行為を指します。

これに該当する行為の例として以下のものが挙げられます。

※1 資金決済法63条の10参照。

※2 以下に示す金融商品取引法上の規定内容および条文番号は、本法による改正後のものです。なお、改正後の金融商品取引法の規定については以下を参照。
<https://www.sangiin.go.jp/japanese/joho1/kousei/gian/221/meisai/m221080221057.htm>

※3 資金決済法2条15項。

※4 金融商品取引法28条5項、同法2条8項18号から25号まで。

※5 資金決済法2条16項、同法63条の2。

※6 金融商品取引法2条9号、同法29条。

- **51% 攻撃**：攻撃者がブロックチェーンのコンセンサス形成能力（例：計算能力やステーク量）の過半数を支配し、取引の承認・拒否やチェーンの書き換えを行う攻撃
- **二重支払を目的とするチェーン再編成の誘発**：攻撃者が秘密裏に別のチェーンを構築し、後から正規チェーンに置き換えることで、既に使用した暗号資産を再び利用可能にする攻撃
- **コンセンサス形成の妨害**：ネットワークの正常な運営を妨げることを目的として、ノード間の合意形成プロセスを阻害し、取引の確定やブロック生成を遅延・停止させる攻撃
- **ノード間通信の阻害**：ネットワークの正常な運営を妨げることを目的として、ノード同士の通信を妨害・遮断し、ネットワークの同期や取引・ブロック情報の伝播を妨げる攻撃
- **大量トランザクション送信によるネットワーク混雑の誘発**：大量の取引を送信してネットワーク資源を消費させ、取引処理の遅延や手数料の高騰を引き起こす攻撃
- **スマートコントラクト、ブリッジ、オラクル等への攻撃**：コードの脆弱性や外部データ連携機能を悪用し、資産の不正取得、価格操作、誤作動を引き起こす攻撃

2 ブロックチェーンに対する攻撃の法規制上の位置付け

(1) ブロックチェーンに対する攻撃の評価

不公正取引と評価されるブロックチェーンに対する攻撃について、暗号資産取引業を行う金融商品取引業者が適切な対応を行わない場合、レピュテーションの深刻な悪化が懸念されます。もっとも、ブロックチェーンに対する攻撃は、それ自体が一律に独立した不公正取引の類型として明示されているわけではありません。したがって、その規制上の評価は、攻撃の態様、目的、価格形成への影響、関連売買の有無等を踏まえ、関連する金融商品取引法上の概念に照らして判断されることになる想定されます。

なお、2026年9月時点においては改正後の金融商品取引法の不公正取引関連の規定は施行されておらず、裁判所による判例や監督官庁による公定解釈も示されていないことから、以下では規制上の文言に照らした一般論を示すにとどめます。

(2) 金融商品取引法上の各禁止行為への該当性

金融商品取引法上の禁止行為として、「暗号等資産の売買〔略〕その他の取引又はデリバティブ取引等〔略〕について、不正の手段、計画又は技巧をすること」（金融商品取引法171条の3第1項）が示されています。このうち「不正の手段」はブロックチェーンに対する攻撃に関連する余地があると考えられます。「不正の手段」という文言からはどのような行為が禁止されているかが必ずしも明確に読み取れるわけではないものの、同様の禁止規定^{※7}が設けられている有価証券の取引に関する判例においては、『不正の手段』とは、有価証券の取引に限定して、それに関し、社会通念上不正と認められる一切の手段をいう^{※8}として、もっぱら社会通念によって禁止行為への該当の有無が判断されています。仮に同様の判断が暗号資産に関する不公正取引規制においても下されるのであれば、社会通念上、ブロックチェーンに対する攻撃が暗号資産の取引に関して不正と認められる手段と評価される限り、本規定による禁止の対象と評価され得ると考えられます。

このほか、ブロックチェーンに対する攻撃が、それを取り巻く事情によって、「偽計」（金融商品取引法171条の4）等の各種概念に該当するか否かについては、今後の判断の蓄積が期待されます。

3 暗号資産取引業を行う金融商品取引業者に求められる実務対応

(1) 管理態勢の整備

ブロックチェーンに対する攻撃に起因するリスクに対処するためには、まず管理態勢の整備が求められます。

求められる対応の例として、①ブロックチェーンに対する攻撃に起因する不公正取引の発生リスクをリスク管理規程に明記すること、②システムリスク管理部門と市場監視部門との情報連携プロセスを明確化すること、③重大事案に係るエスカレーションルールを整備すること、④経営レベルでの報告・意思決定体制を明確化することが挙げられます。

(2) 取扱暗号資産の審査・評価

暗号資産は、その技術的なセキュリティ構造やネットワークの規模が多様であり、ブロックチェーンに対する攻

※7 金融商品取引法157条1項及びその前身となった証券取引法58条1号。

※8 最判昭和40年5月25日集判155号831頁。

撃のリスクは暗号資産の銘柄ごとに大きく異なることから、取扱暗号資産について適切な審査・評価を行うことも重要です。

求められる対応として、①新規取扱審査項目にブロックチェーンに対する攻撃への耐性を含めること、②既存取扱銘柄について定期的な再評価を実施すること、③海外での攻撃事例、取引停止事例、チェーン再編成履歴等を継続的に把握すること、④銘柄ごとに危機発生時の対応方針および施策を定めることが挙げられます。

(3) 市場監視およびオンチェーン監視の高度化

市場監視およびオンチェーン監視の高度化を図ることも有効です。

求められる対応の例として、①市場アラート（例：価格急変、出来高急増、スプレッド拡大）やオンチェーンアラート（例：承認遅延、ブロック停止、チェーン再編成、

大口移転）を設定すること、②市場データとオンチェーンデータの相関分析を実施すること、③疑義の生じた口座と外部ウォレットの関係把握に向けた分析手法を整備することが挙げられます。

4 おわりに

暗号資産市場における攻撃類型は多様であり、現時点では過去事例の蓄積も十分とはいえません。事業者においては、ブロックチェーンに対する攻撃をサイバーセキュリティ上の問題としてのみ取り扱うのではなく、総合的なリスク管理の対象と位置付けた上で対応を進めることが重要です。今後、暗号資産市場における実務の高度化が進む中で、こうした統合的な管理態勢の整備は、事業の継続や市場の信頼性の確保の観点から一層重要になるものと考えられます。

竹内 秀輝（たけうち ひでき）

PwC Japan 有限責任監査法人 ガバナンス・リスク・コンプライアンス・アドバイザリー部 パートナー

監査法人で保険会社に対する監査業務および各種アドバイザリー業務を幅広く経験した後、2011年から2014年にかけて、金融庁監督局保険課および総務企画局総務課国際室で勤務。金融庁在籍期間中は、保険監督者国際機構（IAIS）のメンバーとして国際保険規制に関する検討に携わった他、国内外の監督カレッジへの参画を通じたクロスボーダーでの監督にも従事。現在、規制およびコンプライアンス領域のアドバイザリー業務を金融機関等に提供するほか、テクノロジー活用によるコンプライアンス業務変革関連サービスを主導している。

メールアドレス：hideki.h.takeuchi@pwc.com

安嶋 建（あじま たつる）

PwC Japan 有限責任監査法人 ガバナンス・リスク・コンプライアンス・アドバイザリー部 マネージャー

金融系シンクタンク、大学（教員）、ITベンダー系戦略コンサルティングファーム、監査法人系コンサルティングファームを経て、2022年9月に入所。現在は主として金融機関向け規制対応支援業務を担当。博士（法学）Ph.D. in Law.

メールアドレス：tatsuru.ajima@pwc.com